Network Device Interpretation # 202407

Expansion of MOD_FW Scope

Status: ☒ *Active* □ *Inactive*

Date: *29-Jul-2024*

End of proposed Transition Period (to be updated after TR2TD process): *29-Jul-2024*

Type of Change: ☒ Immediate application □ Minor change □ Major change

Type of Document: ☒ *Technical Decision* □ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* □ *Network iTC*

Affected Document(s): *FWMod v1.4e*

Affected Section(s): *multiple*

Superseded Interpretation(s): *None*

Issue:

Issue: Expansion of MOD_FW Scope

The current PP-Module for Stateful Traffic Filter Firewalls (MOD_FW) is written in such a way that suggests it is only applicable to a device which sits between two networks. Section 1.1.2 (PP-Module TOE Overview) of MOD_FW states:

Such products are generally boundary protection devices, such as dedicated firewalls, routers, or perhaps even switches designed to control the flow of information between attached networks.

Additionally, section 4.1.1 (Threats: Unauthorized Disclosure of Information) states:

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices, then those internal devices may be susceptible to the unauthorized disclosure of information.

We are seeking clarification on whether the intent of MOD_FW can also be interpreted in such a manner that a TOE with internal or “East-West” firewall capabilities could be evaluated under this PP-Module. In other words, a firewall for traffic between two internal entities, rather than between an internal and external entity as is done with traditional firewalls. MOD_FW clearly allows external (North-South) firewalls but the permissibility of evaluating East-West firewalls is ambiguous.

Specifically, the proposed TOE in question would be a “Type 2” vND where the TOE is a hardware appliance running a VM hypervisor and multiple VMs. These VMs could communicate with each other through an internal LAN or with other entities inside the protected network. The TOE has an internal firewall which filters traffic between VMs which reside within the TOE boundary, or between a VM within the TOE and an external endpoint. As of now, it is the CCTL's belief that the proposed TOE is capable of meeting all of the MOD_FW Modified and Mandatory SFRs aside from the fact that the endpoints of the monitored traffic are "a VM inside the TOE" and "an entity on the internal network" rather than "an entity on the external network" and "an entity on the internal network."

In addition to the PP-Module parts cited above we believe that section 1.1.3 would have to be amended (or at least interpreted in a manner where East-West connectivity can still be considered to represent two networks) since it states the following:

A Stateful Traffic Filter Firewall is a device composed of hardware and software that is connected to two or more distinct networks and has an infrastructure role in the overall enterprise network.

If this was acceptable, the Supporting Document (SD) would need to be updated since it currently has numerous references to traffic flowing "through" the TOE. In the use case we are proposing, traffic would be originating from or terminating in the TOE.

Resolution:

The focus of MOD_FW is on devices that are filtering pass-through traffic but MOD_FW was not intended to be applied to devices that are only filtering traffic between TOE components. No changes will be applied to the FW Module.

Rationale:

see Resolution section

Further Action:

None

Action by Network iTC:

None